

United States District Court

for the
Western District of New York

United States of America

v.

Case No. 25-MJ-1270

SHAWN DEMMICK

Defendant

CRIMINAL COMPLAINT

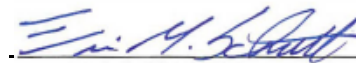
I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about December 17, 2024, in the Western District of New York, and elsewhere, the defendant, **SHAWN DEMMICK**, knowingly distributed any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

All in violation of Title 18, United States Code, Section 2252A(a)(2)(A).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.



Complainant's signature

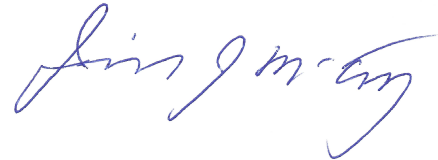
ERIC SCHMIDT
TASK FORCE OFFICER
FEDERAL BUREAU OF INVESTIGATION

Printed name and title

Sworn to before me telephonically.

Date: March 21, 2025

City and State: Buffalo, New York



Judge's signature

HON. JEREMIAH J. MCCARTHY
UNITED STATES MAGISTRATE JUDGE

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I. INTRODUCTION

I, ERIC SCHMIDT, after being duly sworn, depose and state as follows:

1. I am a Police Detective with the Town of Tonawanda, New York Police Department. I have been a Police Officer since January of 2002. I am currently assigned as a Task Force Officer with the Federal Bureau of Investigation (FBI), Buffalo Field Office, Child Exploitation Task Force, which targets individuals involved in the online sexual exploitation of children. I have been a Task Force Officer since April of 2017. As part of these duties, I have become involved in the investigation of suspected violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography in various forms of media, including computer media.

2. This affidavit is made in support of a criminal complaint and arrest warrant charging **SHAWN DEMMICK** with a violation of Title 18, United States Code, Section 2252A(a)(2)(A) (distribution of child pornography).

3. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, and on my experience and training. Because this affidavit is being submitted for the limited purpose of securing a criminal

complaint and arrest warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that **SHAWN DEMMICK** has violated Title 18, United States Code, Section 2252A(a)(2)(A) (distribution of child pornography).

II. PROBABLE CAUSE

4. On December 31, 2024, MediaLab/Kik sent a Cybertip (204191176) to NCMEC reporting that on December 19, 2024, someone reported a user who had uploaded or shared eight files depicting child pornography with another user or group of users using the Kik mobile application. The screen/username of the suspect listed in the report was “sirbannedalot”, and the associated email address for the sirbannedalot Kik account was listed as “sirbannedalot@yahoo.com”. Kik reported that the IP address that was associated with the account at the time of the uploads of child pornography was 172.56.6.200.¹ . A MediaLab/Kik representative had reviewed the files in the report.

5. NCMEC referred the Cybertip to the New York State Police (NYSP) Internet Crimes Against Children (ICAC) Task Force, which opened case #:2025-0182 on or about January 27, 2025. On February 5, 2025, the NYSP ICAC Task Force sent a request to the Department of Homeland Security for an administrative subpoena to obtain subscriber information and IP address logins for Yahoo account user, “sirbannedalot@yahoo.com.” A

¹ These uploads had different port numbers because of a difference in time for the uploads. A port is a virtual point used by the computer's operating system to identify end-to-end network connections. Each port is associated with a specific application on the computer. While IP addresses enable messages to be sent and received from specific devices, port numbers identify the specific applications within those devices.

subpoena was sent to Yahoo Inc. requesting that information. Yahoo responded with the following information:

- **Target:** sirbannedalot
- **Account Status:** Active
- **Registration IP Address:** 2607:fb91:2633:a02:44e:a69a:63bd:fdb2 (port: 60888)
- **Registration Date:** 2024-12-17 18:44:27 Z
- **Full Name:** Tim Davis
- **Recovery Phones:** +1716830[xxxx]
- **Verified on:** 2024-12-17 18:44:27 Z

6. On February 12, 2025, the Department of Homeland Security sent an administrative subpoena to T-Mobile USA Inc., requesting subscriber information for the IP address, “2607:fb91:2633:a02:44e:a69a:63bd:fdb2 port: 60888” on December 17, 2024 at 6:44:27 UTC. T-Mobile responded with the following information:

- T-Mobile hereby objects to the referenced legal demand and is unable to respond to your request for the following reason(s): No records were found.

7. On or about February 19, 2025, the Department of Homeland Security sent an administrative subpoena to T-Mobile USA, Inc. to obtain subscriber information for the telephone number 716-830-xxxx (i.e., the phone number associated with sirbannedalot@yahoo.com) from 02/18/2024 through 02/18/2025. T-Mobile responded with the following information:

- **Customer Number:** 716-830-xxxx
- **Customer Name:** SHAWN DEMMICK
- **Subscriber Name:** SHAWN DEMMICK
- **Service Address:** xxxx, Tonawanda, NY 14150
- **Billing Address:** xxx, Tonawanda, NY 14150
- **Service Start Date:** 03/15/2014 7:00

8. Kik also disclosed basic subscriber data and recent IP addresses associated with Kik account “sirbannedalot.” The following was included with that data:

- **First Name:** sirbannedalot
- **Last Name:**
- **Email:** sirbannedalot@yahoo.com (unconfirmed)
- **Username:** sirbannedalot
- Phone make on 12/19/2024: Samsung (no model or IMEI number)
This account showed multiple logins between 12/19/2024 and 12/20/2024 including IP address 172.56.6.200(various port numbers).

9. On March 18, 2025, your affiant received NCMEC Cybertip 204191176 from the NYSP ICAC Unit via the ICAC Data System (Case #: 2025-0182) and reviewed the associated case files.

10. I reviewed the files provided in NCMEC Cybertip 204191176 that MediaLab/Kik provided. According to the Cybertip, an individual from MediaLab/Kik did review the contents of the uploaded files. The table below describes certain observations in four of the files. It should be noted that three of the files had different file names but contained the same video. Based on my training and experience, I believe these videos contain child pornography as defined in under Federal Law.

Photo Name	Description
Fe9fe2d8-64b7-4b5f-9cba-9fdbb40cfd6b.mp4	A video approximately 2 minutes in length, depicting a prepubescent minor female approximately 7-9 years of age with brown hair. The minor female victim is sitting on a toilet and appears to be crying. The minor female victim is performing oral sex on an adult male. At the end of the video the minor female victim places the male's penis back into his underwear.

Da8e2ecf-1bac-4b21-9893-2431f247b13e.mp4	A video approximately 10 seconds in length, depicting a prepubescent minor female approximately 5-7 years of age. The minor female victim is wearing a light blue tank top and is holding an adult male's erect penis and is licking it with her tongue. The minor female victim then sticks her tongue out as the male ejaculates into the minor female victim's mouth. The video concludes with the minor female victim kissing the male's penis.
C0043bde-678f-47d5-b69f-275f2629b3cc.mp4	A video approximately 2 minutes in length, depicting a prepubescent minor female approximately 4-6 years of age. The minor female is wearing a light blue pajama shirt. The minor female victim is sitting in front of an adult male with her legs crossed. The adult male is manually stimulating his erect penis with his hand as the minor female victim leans over the penis. The minor female victim then begins sucking on the male's penis and uses both hands to manipulate it as well. The video concludes with the male ejaculating and the minor victim placing her mouth back on his penis as he does.
1ab608dd-fae0-48cd-a875-883377488129.mp4	A video approximately 38 seconds in length, depicting a minor female victim approximately 9-11 years of age. The minor female is wearing a white colored t-shirt and a large overweight adult male is standing next to her with his erect penis out of his pants. The minor female victim is performing oral sex on the male. At one point the male puts his hand on the back of the minor female victim's head forcing her mouth further onto his penis. The words, "Telegram:PeachLeaks" are seen in the top left side of the video.

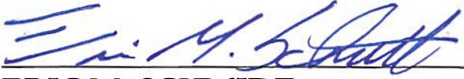
11. Based on the facts set forth above, on March 21, 2025, during the interview with **SHAWN DEMMICK** outside of his place of employment, **SHAWN DEMMICK** admitted to sending and receiving child sexual abuse material (CSAM)² on Kik, Telegram, and through Mega.NZ links. **SHAWN DEMMICK** admitted that he believed that he had between three hundred and four hundred videos of CSAM on his Samsung cellular device

² In this affidavit, I intend the term "child sexual abuse material," or "CSAM," to have the same meaning as the term "child pornography," as the latter term is defined in Title 18, United States Code, Section 2256(8). I use the term "CSAM" interchangeably with the term "child pornography." Thus, my conclusion that a particular image or video qualifies as "CSAM" necessarily means that I believe that the image qualifies as "child pornography," as that term is defined under federal law.

within the Mega.NZ account. **SHAWN DEMMICK** did consent to a search of the Mega.NZ account, which passcode was “6492”. Further review of the Mega.NZ account revealed approximately 350 possible CSAM videos, one of which was found to be one of the videos Kik had provided in the Cybertipline case. That video is described above as “Da8e2ecf-1bac-4b21-9893-2431f247b13e.mp4” and had a title in the Mega.NZ account of “VID_20241217_162226_098.mp4.”

III. CONCLUSION

Based upon the above information, I assert that probable cause exists to believe that **SHAWN DEMMICK** has violated Title 18, United States Code, Section 2252A(a)(2)(A) (distribution of child pornography). I therefore request that the Court issue the requested criminal complaint and arrest warrant


 ERIC M. SCHMIDT
 Task Force Officer
 Federal Bureau of Investigation

Sworn to and subscribed telephonically

this 21st day of March, 2025.



HON. JEREMIAH J. MCCARTHY
 United States Magistrate Judge